AMENDMENTS TO THE CLAIMS

Please amend the claims as follows:

1. (Currently Amended) A computer-implemented method for training a ~~computer code~~ database intrusion detection system in real time, said method comprising the steps of:

observing, in real time, commands that are accessing the ~~computer code~~ database; and

deriving from said commands, in real time, a set of acceptable commands.

2. (Canceled)

3. (Original) The method of claim 2 wherein the commands are SQL commands.

4. (Currently Amended) The method of claim 1 wherein at least one observed command is from the group of commands comprising a query, an add, a delete, and a modify.

5. (Original) The method of claim 1 wherein the deriving step comprises:

grouping the commands into categories; and

updating statistical information pertaining to the categories in real time.

6. (Currently Amended) The method of claim 5 wherein the categories comprise at least one category from the group of categories comprising:

canonicalized commands;

dates and times at which commands access the computer code;

logins of users that issue commands;

identities of users that issue commands;

departments of users that issue commands;

applications that issue commands;

IP addresses of issuing users;

frequency of issuing commands by users;

identities of users accessing a given field within the ~~computer code~~ database;

times of day that a given user accesses a given field within the ~~computer code~~ database;
fields accessed by commands;
combinations of fields accessed by commands;
tables within the ~~computer code~~ database accessed by commands;
combinations of tables within the ~~computer code~~ database accessed by commands.

7. (Original) The method of claim 5 wherein:
the categories comprise canonicalized commands; and
each category is a command stripped of literal field data.

8. (Original) The method of claim 1 wherein the observing step comprises at least one of:
real-time auditing; and
in-line interception.

9. (Currently Amended) The method of claim 8 wherein the observing step comprises real-time auditing; and at least one of the following is used to extract the commands for observation:
an API that accesses the ~~computer code~~ database;
code injection;
patching;
direct database integration.

10. (Currently Amended) The method of claim 8 wherein the observing step comprises in-line interception; and at least one of the following is interposed between senders of the commands and the ~~computer code~~ database:
a proxy;
a firewall;
a sniffer;

11. (Original) The method of claim 1 wherein:

during the deriving step, suspicious activity is tracked; and

subsequent to the deriving step, the suspicious activity is reported to a system administrator.

12. (Original) The method of claim 1 wherein a duration of performing the deriving step is determined by statistical means.

13. (Currently Amended) The method of claim 1 further comprising, subsequent to the deriving step, an operational step in which commands that are accessing the ~~computer code~~ database are compared against the set of acceptable commands.

14. (Currently Amended) The method of claim 13 wherein a command that is accessing the ~~computer code~~ database during the operational step that does not match a command in the set of acceptable commands is flagged as suspicious.

15. (Currently Amended) The method of claim 14 wherein, when a command is flagged as suspicious, at least one of the following is performed:

an alert is sent to a system administrator;

the command is not allowed to access the ~~computer code~~ database;

the command is allowed to access the ~~computer code~~ database, but the access is limited;

the command is augmented;

a sender of the command is investigated.

16. (Currently Amended) A computer-readable medium containing computer program instructions for training a ~~computer code~~ database intrusion detection system in real time, said computer program instructions performing the steps of:

observing, in real time, commands that are accessing the ~~computer code~~ database; and

deriving from said commands, in real time, a set of acceptable commands.

17. (Original) The computer-readable medium of claim 16 wherein the deriving step comprises:

grouping the commands into categories; and

updating statistical information pertaining to the categories in real time.

18. (Original) The computer-readable medium of claim 17 wherein:

the categories comprise canonicalized commands; and

each category is a command stripped of literal field data.

19. (Currently Amended) The computer-readable medium of claim 16 further comprising, subsequent to the deriving step, an operational step in which commands that are accessing the ~~computer code~~ database are compared against the set of acceptable commands.

20. (Currently Amended) Apparatus for training a ~~computer code~~ database intrusion detection system in real time, said apparatus comprising:

a training module adapted for observing, in real time, commands that are accessing the ~~computer code~~ database, and for deriving from said commands, in real time, a set of acceptable commands; and

coupled to the set of acceptable commands, a comparison module for comparing commands that access the ~~computer code~~ database during an operational phase with commands in the set of acceptable commands.

21. (New) A computer-readable medium containing computer program instructions for providing a database intrusion detection system, said computer program instructions performing steps comprising:

observing commands that are accessing a database during a training phase, the commands comprising literal field data;

stripping the commands of literal field data to produce commands in canonical forms;

grouping the commands responsive to the commands' canonical forms;

generating a set of acceptable commands responsive to the grouped commands;

comparing commands that access the database during an operation phase with commands in the set of acceptable commands; and

flagging as suspicious a command that accesses the database during an operation phase responsive to a determination that the command is not in the set of acceptable commands.